UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/829,763	04/10/2001	Osamu Shibata	29288.0400	9593

20322 7590 12/26/2006

SNELL & WILMER
400 EAST VAN BUREN
ONE ARIZONA CENTER
PHOENIX, AZ 85004-2202

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/26/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/829,763	SHIBATA ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8 and 9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8 and 9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

In response to an election/restriction requirement, applicant responded on 10/5/2006, electing group I (claims 1, 3-6, and 8-9). Claims 2 and 7 were cancelled. As no arguments with respect to the restriction requirements were presented, the election is treated as an election without traverse and made FINAL.

Response to Arguments

Applicant's remarks with regards to the pending claims that were previously submitted on 7/6/2006 were fully considered, but were not persuasive. Applicant argues that the specification has several descriptions of the term "initial state", thus the term is clearly defined. The examiner respectfully disagrees. While the term is used within the context of various examples, there is no disclosure in the specification which instructs one reading the application to always apply a specific meaning to the term, thereby excluding any other meaning. As such, there is no prohibition towards applying a broader, yet reasonable definition to the term as would be understood by one of ordinary skill in the art when examining the claims. In this case, the examiner has interpreted "initial state" as referring to any state prior to a current state.

Applicant further remarks are with regards to the limitation "wherein the content key storage section is in initial state immediately after at least one of a power-on of the decryption device and the decryption device is reset". Applicant essentially argues that the prior art of record does not teach this limitation and that this added limitation makes it clear that "initial state" as used in the claims is different from the examiner's interpretation. The examiner respectfully disagrees. One of ordinary skill would

understand that a decryption device (or any other computing device) is a state machine, thus the device and its component always has certain states. As such, the content key storage section always has state. When compared to a current state, any state previous to the current state can be considered an initial state. When the device is powered off, the device and the components which makes up the device have state. When first powered on or reset, the device and the components which makes up the device have state. If the state of the content key storage section after it was turned on or reset is different than a later state, i.e. a current state or future state, the state of the content key storage section can be considered an initial state as compared to the later state. Note also in referring to "an initial state immediately after at least one of a power-on of the decryption device and the decryption device is reset", the claim implies that there can be more than one state that is considered "an initial state".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-6, and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al (US 5,923,754) in view of Venkatesan et al (US 6,801,999), herein Ven, and further in view of Sims (US 2002/0016919).

Claims 1, 3-6, and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al (US 5,923,754) in view of Venkatesan et al (US 6,801,999), herein Ven, further in view of Sims (US 2002/0016919) and further in view of applicant's admittance of prior art.

Claims 1 and 6:

As per claim 1, Angelo discloses the limitations of:

1. An internal-key storage section adapted to store an internal key (Fig 2, items 42 and 44; col 3, lines 50-58; and col 4, lines 31-33).
2. A content-key storage section adapted to store content-keys (Fig 3, items 62 and 64; col 3, lines 50-58; and col 4, lines 41-67).
3. An operation section, the operating section including:
    a. A first decrypting section adapted to, when an encrypted content-key is input to the operation section, decrypt the encrypted content-key using the internal-key so as to obtain a content-key and store the content-key in the content-key storage section (Fig 3, item 66; col 3, lines 58-62; and col 4, lines 59-61).
    b. A second decrypting section adapted to, when an encrypted content is input to the operation section, decrypt the encrypted content using the current value of the content-key storage section as a content-key so as to obtain a first output data and output the first output data to the outside of the decryption device (Fig 3, items 68-72; col 3, lines 58-62; and col 4, lines 61-67).

As per the limitation wherein the content key storage section is in an initial state immediately after at least one of a power-on of the decryption device and the decryption device is reset, one of ordinary skill in the art should appreciate that computing devices, including the decryption device being claimed are state machines, thus always has state. One can always consider the state of the content key storage section as being in an initial state immediately after at least one of a power-on of the decryption device and the decryption device is reset because it is one of the first states defined for the content key storage section during active operation of the device.

Angelo does not disclose a determination section adapted to determine whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different. Angelo does not disclose the decryption of the encrypted content also being dependent on the determination section determining that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different.

However, the examiner notes that applicant's specification does not explicitly define what is the "initial state". The examiner submits that in the broadest, reasonable sense, any state of the content-key storage section can be considered the "initial state" as compared to a later point in time. The examiner assumes the state of the storage section that is most recent in time is the "current state" and any state prior to the most recent as an "initial state" including the state immediately after at least one of a power-on of the decryption device and the decryption device is reset.

Ven discloses using keys which expires after a given interval of time (col 7, lines 49-52). Ven discloses a client PC, i.e. decryption device, being unable to access protected objects/content until a new valid key was obtained (col 8, lines 37-56). One of ordinary skill should appreciate that when a new key has been obtained, the state of the key storage section would change from what it was before, i.e. the initial state. Sims discloses checking for keys which have been revoked/expired or banned (p10, paragraphs 108-109).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill to incorporate Ven and Sims's teaching with Angelo's invention according to the limitations recited in claim 1. Note that within the context of the combination invention of Angelo, Ven, and Sim, the examiner is considering state at the point in time in which the content key storage section has initial key (i.e. K as per Ven's teachings) to be the initial state. When this key is replaced (i.e. with K' as per Ven's teachings), the content key storage section is in a current state. One of ordinary skill would have been motivated to incorporate Ven's teachings because it would allow Angelo's invention to be more secure against piracy by protecting against "break-once-run-everywhere" (BORE) attacks (Ven: col 5, lines 16-21). One of ordinary skill would be motivated to incorporate Sims's teachings as it would allow the combination invention of Angelo and Ven to determine when someone is attempting to use an expired or banned key to decrypt media content. Note that in Ven's invention, there needs to be a way to determine if a key being use has expired or not; Sims's teachings provides for the solution to this need. Note that as per Sims's teachings, if a decryption device was still

using a key that had expired or been banned, then the content-key storage section's state had not changed from its initial state. One of ordinary skill should appreciate that decryption of encrypted content is dependent on having updated and valid keys, so decryption would fail.

Alternatively, as per the limitation wherein the content key storage section is in an initial state immediately after at least one of a power-on of the decryption device and the decryption device is reset, the examiner also notes that applicant admits that the limitation was well known in the art at the time applicant's invention was made (specification: p3, line 31-p4, line 9). It would have been obvious to one skilled in the art to incorporate the limitation within the combination invention of Angelo, Ven, and Sims because it is a conventional feature of decryption devices common to many prior art decryption devices.

Claim 6 is substantially similar to claim 1 except it is directed towards a method for decrypting encrypted content, the method being performed by the device of claim 1. It is rejected for substantially the same reasons given for claim 1.

Claim 3:

As per claim 3, Angelo further discloses:

1. A mutual authentication section adapted to determine whether or not a mutual authentication has been made between the mutual authentication section and a storage device which is located outside the decryption device, the encrypted content-key being stored in the storage device (col 4, lines 42-52).

2. Wherein the second decrypting section is adapted to decrypt the encrypted content when the mutual authentication section determines that the mutual authentication has been made (col 4, lines 57-67).

Claims 4 and 8:

As per claim 4, Angelo further discloses:

1. The internal-key storage section is adapted to store a plurality of internal-keys (col 4, lines 31-33 and Fig 2).
2. The internal-key storage section is adapted to select one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption section (Fig 3). *Note that Sims also discloses this limitation (p9, paragraph 97).*

Claim 8 is substantially similar to claim 4 except it is directed towards a method which utilizes the decryption device of claim 4 to perform the intended use of the device of claim 4. It is rejected for substantially the same reasons given for claim 4.

Claims 5 and 9:

As per claims 5, Ven further discloses the second decrypting section is further operable to prevent decryption of the encrypted content (col 7, lines 48-51 and col 8, lines 46-51). Ven does not explicitly disclose the decryption is dependent on the determination section determining that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same. However, as stated previously, applicant's specification does not define what is the

"initial state". The examiner interprets any state of the content-key storage section as the initial state as compared to a later state in time. One of ordinary skill should appreciate that Ven keeping the decryption device from processing content if the value in the key storage section is the same (col 8, lines 46-51), i.e. if the key storage section has not yet obtain a key that has not expired, reads on the above limitation. The technique of how Ven can make this determination is further disclosed by Sims (p10, paragraph 108). One of ordinary skill would have been motivated to incorporate Ven and Sims's teaching within Angelo's invention for the same reasons given in claim 1.

Claim 9 is substantially similar to claim 5 except it is directed towards a method which utilizes the decryption device of claim 5 to perform the intended use of the device of claim 5. It is rejected for substantially the same reasons given for claim 5.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100